UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,571	08/02/2006	Estelle Transy	18394017US1RVLPA61423US	2383

26221 7590 08/28/2009

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/28/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/565,571	TRANSY ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/17/2009 has been entered. Claims 21, 22, 23, 25, 26, 27, 28, 29, 30, and 31 have been amended. Claims 21-31 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 21-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stenberg (International Publication No. WO 01/3666 (cited from IDS)) in view of Rezaiifar et al. (US Patent Publication No. 2003/0055964 and Rezaiifar hereinafter).

2. As to claim 21, Stenberg teaches a method for authenticating a user for access to at least two entities of a data transmission network via a terminal, each data entity having an associated authentication device, the authentication devices being independent of each other (i.e., ...teaches the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer [pg. 4, lines 20-30. Those skilled in the art would recognize that the overlaying network layer and the radio access network layer are two authentication means that perform individual authentication operation (e.g., independent authentication operation) and that these layer are separate) method comprising::

a random number is transmitted to the terminal (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]),

data for authenticating the user to the two entities of the network is calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user (i.e., ...teaches a computing first ciphering key from a random challenge number [claim 5]),

the terminal inserts, in an access request, data for identifying the user to said entities of the network and the calculated authentication data, and transmits the access request to an access controller (i.e., ...teaches an authentication triplet of the GSM as part of authentication parameters [pg. 4, lines 25-35]. Those skilled the art would recognize such authentication parameter as part of a formal request therefore having been inserted by requesting entity),

the access controller transmits, to each of the authentication devices for the two entities, a respective authentication request containing the identification data and the distinct set of inserted data for authenticating the user to the respective entity of the network, contained in the access request (i.e., ... teaches receiving authentication parameter [claim 16; pg. 18, lines 13- 15]),

the authentication devices of the entities carry out a user authentication procedure [fig, 3; pg, 12, lines 30-36], on the basis of user identification and authentication data (pg, 8, lines 11-25),

contained in the authentication requests (i.e., ...teaches receiving authentication parameter [claim 16; pg. 18, lines 13-15]),

authentication reports containing results of the authentication procedures carded out by the authentication devices of each of said two network entities are transmitted to the terminal (i.e., ...teaches sending results of authentication [pg. 12, lines 35-36]).

Stenberg does not expressly teach claim limitation element of wherein the inserted data for identifying the user comprises a distinct set of data for each of the two entities.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Stenberg as introduced by Rezaiifar. Rezaiifar discloses: the inserted data to identifying the user comprise a distinct set of data for each of the two entities (to provide a set of data inserted into a request for purposes of sender identification [par. 40]).

Therefore, given the teachings of Rezaiifar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Stenberg by employing the well known features of inserting user identification data into a request disclosed above by Rezaiifar, for which user authentication will be enhanced [par. 40]).

3. As to claim 22, Stenberg teaches a method characterized in that it includes a preliminary step in which the terminal establishes a connection with a specialized server via the network [fig. 3], where the random number is generated and transmitted to the terminal by the specialized server when the connection has been established (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]).

4. As to claim 23, Stenberg teaches a method characterized in that the access request transmitted by the terminal is transmitted to the specialized server which inserts therein the random number used to calculate the authentication data (i.e., ...teaches a

computing first ciphering key from a random challenge number [claim 5]), the access request is then transmitted to the access controller which inserts the random number into the authentication requests transmitted to the authentication devices for the two entities (i.e., ...teaches a AuC generates a random challenge [pg. 8, lines 10-20] ... further teaches a AuC is either a separate unit or integrated into the HLR [pg. 8, lines 10-20]).

5. As to claim 24, Stenberg teaches a method characterized in that the identification data inserted into the access request is in the form: "IdA@DomainA" in which: "IDA" represents the identifier for identifying the user to the network entity (i.e., ... teaches initial authentication is based on the authentication triplet of GSM [pg. 4, lines [pg. 4, lines 27-30] Those skilled in the art would recognize user identity is inherent to the authentication triplet of the GSM), "DomainA" represents the identifier of the network entity in the network (i.e., ... teaches initial authentication is based on the authentication triplet of GSM [pg. 4, lines [pg. 4, lines 27-30]), with the access controller determining the entities to whom the authentication requests will be transmitted on the basis of the "DomainA" identifiers of the network entity contained in the access request (i.e., ... teaches initial authentication is based on the authentication triplet of GSM [pg. 4, Those skilled in the art would recognize user identity is inherent to the authentication triplet of the GSM).

6. As to claim 25, Stenberg teaches a user terminal capable of accessing, by means of the access network, at least two entities connected to a data transmission network [fig. 3]:

each data entity having an associated authentication device, the authentication devices being independent of each (i.e., ...teaches the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer [pg. 4, lines 20-30. Those skilled in the art would recognize that the overlaying network layer and the radio access network layer are two authentication means that perform individual authentication operation (e.g., independent authentication operation) and that these layer are separate):

characterized in that it includes:

a transmitting apparatus that transmits access requests at least two entities of the network [fig. 3], which requests contain data for identifying and authenticating the user to the network entity and each request being distinct [pg. 8, lines 10-20];

a receiving apparatus that receives a random number when a connection with the network is established (i.e., ...teaches restoring random challenge number from translated parameter. Said translated parameter being transmitted [pg. 15, lines 20-30],

cryptographic calculating apparatus that applies at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network (i.e., ...teaches a first cipher key from random challenge [pg. 30, lines 30- 35]), and inserting, apparatus that inserts into each transmitted access request, data for identifying the user to each

network entity and the calculated authentication data (i.e., ... teaches translating random challenge number into authentication parameter [pg. 15, lines 20- 25]).

Stenberg does not expressly teach claim limitation element of wherein the calculated authentication data comprises a distinct set of authentication data for each entity.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Stenberg as introduced by Rezaiifar. Rezaiifar discloses: the calculated authentication data comprises a distinct set of authentication data for each entity (to provide a computed authorization data for which includes user identification data [par. 38]).

Therefore, given the teachings of Rezaiifar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Stenberg by employing the well known features of inserting user identification data into a request disclosed above by Rezaiifar, for which user authentication will be enhanced [par. 38]).

7. As to claim 26, Stenberg teaches a terminal characterized in that it includes an external module designed to be connected to each of the user terminals and including a receiving apparatus that receives the random number from the terminal to which it is connected (i.e.,...teaches computing response [pg. 15, lines 30-36]), cryptographic

calculation apparatus that executes the predefined cryptographic algorithm based on the random number (i.e., ...teaches a computing first ciphering key from a random challenge number [claim 5]), and for transmitting, to the terminal, at least one data item for authenticating the user to an entity of the network (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]), obtained by the cryptographic calculations.

8. As to claim 27, Stenberg teaches a access controller, characterized in that it includes a receiving apparatus that receives request for access to at least two entities of a data transmission network coming from user terminal and transmitted via said network [fig. 3], extracting apparatus that extracts, from the access request (i.e., ...teaches restoring challenge number for authentication [pg. 15, lines 25-30]), the data for identifying and authenticating the user to a respective one at least two network entities (i.e., ...teaches the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer [pg. 4, lines 20-30]. Those skilled in the art would recognize that the overlaying network layer and the radio access network layer are authentication mechanisms that perform individual authentication (e.g., independent authentication operation. The overlaying network layer and radio access network layer being the two network entities),

A transmitting apparatus that transmits (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]), to each of the two entities, a respective authentication request containing the data for identifying and authenticating

the user to the two entities, contained in the access request (i.e., …teaches the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer [pg. 4, lines 20-30. Those skilled in the art would recognize that the overlaying network layer and the radio access network layer are two authentication means that perform individual authentication operation (e.g., independent authentication operation) and that these layer are separate).

Stenberg does not expressly teach claim limitation element of wherein the inserted data for identifying the user comprises a distinct set of data for each of the two entities.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Stenberg as introduced by Rezaiifar. Rezaiifar discloses:

the inserted data to identifying the user comprise a distinct set of data for each of the two entities (to provide a set of data inserted into a request for purposes of sender identification [par. 40]).

Therefore, given the teachings of Rezaiifar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Stenberg by employing the well known features of inserting user identification data into a request disclosed above by Rezaiifar, for which user authentication will be enhanced [par. 40]).

9. As to claim 28, Stenberg teaches a access controller characterized in that it also includes means for receiving user authentication reports, transmitted by the entities in response to the authentication requests, and means for transmitting, to the user terminal, and authentication report based on the reports received from the entities (i.e., ...teaches sending results of authentication [pg. 12, lines 35-36] Those skilled in the art would recognize transmitter/receiver relationship within a mobile communication environment).

10. As to claim 29, Stenberg teaches a system for authenticating a user in an attempt to access at least two entities of a data transmission network to which network entities are connected, and which user terminals can access by means of access networks [fig. 3], characterized in that it includes: a user terminal characterized in that it includes [fig. 3]: means for transmitting access requests to an entity of the network, which requests contain data for identifying and authenticating the user to the network entity [fig. 3]; means for receiving a random number when a connection with the network is established [fig. 3], cryptographic calculating means for applying at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network (i.e., ...teaches a computing first ciphering key from a random challenge number [claim 5]), and means for inserting, into each transmitted access request, data for identifying the user to two network entities and the calculated authentication data (i.e., ...teaches a translating

random challenge number into authentication parameter sent to authenticator [pg. 15, lines 20-25]); at least one authentication server for each of the network entities, designed to identify and authenticate the users on the basis of identification and authentication data contained in the access requests received [fig. 3];

an access controller characterized in that it includes means for receiving requests for access to at least two entities of the data transmission network coming from user terminals and transmitted via said network [fig. 3], means for extracting from each of the access requests, the data for identifying and authenticating the user to at least two network entities (i.e., ...teaches restoring challenge number for authentication [pg. 15, lines 25- 30]), means for transmitting, to each of the two entities, a respective authentication request containing the data for identifying and authenticating the user to the two entities, contained in the access request (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]).

Stenberg does not expressly teach claim limitation element of wherein the calculated authentication data comprises a distinct set of authentication data for each entity.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Stenberg as introduced by Rezaiifar. Rezaiifar discloses: the calculated authentication data comprises a distinct set of authentication data for each entity (to provide a computed authorization data for which includes user identification data [par. 38]).

Therefore, given the teachings of Rezaiifar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Stenberg by employing the well known features of inserting user identification data into a request disclosed above by Rezaiifar, for which user authentication will be enhanced [par. 38]).

11. As to claim 30, Stenberg teaches a system characterized in that it also includes a specialized server connected to the network so as to be connected to the user terminals when a connection has been established between the terminal and the network [fig. 3], where the specialized server includes means for generating and transmitting a random number to each of the terminals with which a connection is established (i.e., ...teaches sending an authentication parameter carrying a random challenge [claim 5]), and means for inserting the random number into each of the access requests transmitted by the terminals (i.e., ...teaches a translating random challenge number into authentication parameter sent to authenticator [pg. 15, lines 20-25]).

12. As to claim 31, Stenberg teaches a system characterized in that each entity of the network includes means for storing secret keys of users (i.e., ...teaches deriving a second ciphering key from first ciphering key [pg. 14, lines 10-15]), means for determining the data for authenticating the user to the entity by applying the predefined algorithm to the random number received in a authentication request and to the secret

user key (i.e., ...teaches a computing first ciphering key from a random challenge number [claim 5]), and for comparing the result obtained to the user authentication data received in the authentication request (i.e., ... teaches authentication comparison [pg. 12, lines 30-36]), where the user is properly authenticated by the entity only if the result of the cryptographic calculation obtained is identical to the authentication data contained in the authentication request (i.e.., ... teaches authentication is accepted when values matches [pg. 12, lines 34-36]).

Response to Arguments

Applicant's arguments filed 6/17/2009 have been fully considered but they are not persuasive.

With regards to applicant's argument of Stenberg is deficient in teaching "authentication devices being independent of each", the Examiner contends that Stenberg teaches the authentication using a overlaying network layer in combination with the authentication procedures of the radio access network layer [pg. 4, lines 20-30]. The overlaying network layer and the radio access network layer being the two authentication devices performing independent authentication. Those skilled in the art would recognize that the overlaying network layer and the radio access network layer are two authentication means that perform their own individual authentication (e.g., independent authentication operation).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431